Chapitre II: Architecture des réseaux informatiques

1. Introduction

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés (SNA d'IBM, DECnet de DEC, DSA de Bull, TCP/IP du DoD, ...) et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux hétérogènes si une norme internationale n'était pas établie.

Alors, une normalisation de l'architecture logicielle s'impose. Deux grandes familles d'architectures se disputent le marché. La première provient de l'ISO et s'appelle OSI (*Open System Interconnection*). La deuxième est TCP / IP. Une 3ème Architecture plus récente est UIT-T (Union Internationale des Télécommunications). Il s'agit de l'adaptation du modèle OSI pour prendre en compte les réseaux haut – débit (réseau ATM).

2. Modèle de référence OSI

Le modèle de référence défini par l'ISO est l'OSI (Open System Interconnection). Il permet à des systèmes hétérogènes de s'interconnecter et d'échanger des informations. Il est par conséquent indépendant de la structure et de la technologie des matériels employés. Ce modèle OSI constitue un cadre de référence qui nous permet de comprendre comment les informations circulent dans un réseau. C'est aussi un modèle conceptuel d'architecture de réseau qui facilite la compréhension théorique du fonctionnement des réseaux.

La complexité de conception, de réalisation et de maintenance des logiciels et de l'architecture des réseaux, est maîtrisée grâce à une organisation en couches, chaque couche étant bâtie sur la précédente.

2.1. Principes de fonctionnement de modèle OSI

Le modèle OSI est composé de sept (7) couches, chacune définissant des fonctions particulières du réseau.

Le concept de l'OSI nécessite la compréhension de 3 concepts.

- Le service (N) : Ensemble d'événements et primitives pour rendre au niveau (n+1).
- Le protocole (N) : Ensemble de règles nécessaires pour le service (N) soit réalisé.

- Le point d'accès à un service (N-SAP) : Point situé à la frontière entre les couches (n) et (n+1).

Chaque couche peut interagir uniquement avec les deux couches adjacentes.

Chaque couche (n) offre un certain nombre de services à la couche (n+1) en déroulant un protocole uniquement défini à partir des services fournis par la couche (n-1).

Chaque couche niveau N traite une tâche, un protocole ou un composant matériel, repose sur les couches sous-jacentes, et communique avec les autres couches. Cette communication entre les couches s'effectue au travers d'interfaces définies. En principe, seules deux couches adjacentes peuvent communiquer, dans la mesure où la famille de protocoles utilisée les exploite. Il n'est pas possible de « sauter » une couche. La couche la plus élevée (couche application) est la plus proche de l'utilisateur; la couche inférieure (couche physique) est la plus proche des médias de transmission.

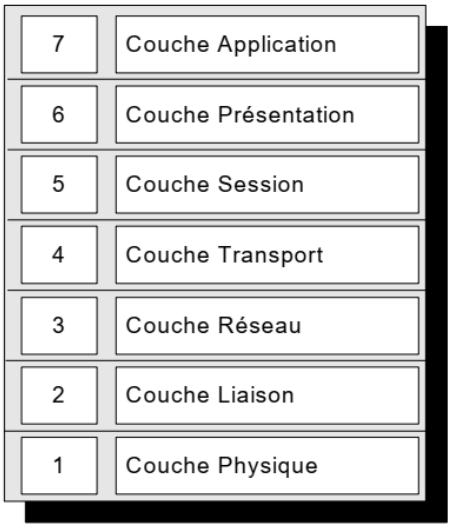


Fig.1. Les sept couches du modèle OSI.

2.2. Couches du modèle OSI

a. La couche physique : La couche physique (Physical layer) assure, comme son nom l'indique, le transport physique de données. Il s'agit de la transmission de signaux électriques, optiques ou de radiofréquences à travers des médias appropriés et tous les détails associés comme les connecteurs, les types de codage ou de modulation, le niveau des signaux, les longueurs d'onde, la synchronisation et les distances maximales.

b. **Couche liaison de données :** Connexion entre entité, Correction des erreurs, partage du support responsable de l'acheminement d'unités de données appelées trames (frames) à partir des paquets (blocs de données) de la couche réseau, à destination de la couche physique en assurant la meilleure qualité de transmission possible. Une trame est une suite structurée de bits.

c. **Couche réseau :** La couche réseau, également appelée couche Internet ou couche IP, accepte et distribue les paquets pour le réseau.

Connexion sur système ouvert (passerelles, ...), Adressage, Routage, Contrôle de flux offre un nombre de services dont un service d'adressage IP (Internet Protocol) permettant d'atteindre son destinataire, un service de routages déterminant un chemin à l'intérieur du réseau maillé et un contrôle du flux pour ne pas saturer le réseau.

d. **Couche transport :** Optimise l'utilisation de la couche réseau et assure le transfert sans erreur des paquets. Elle subdivise en petits blocs les messages longs. Les paquets trop petits sont assemblés en grands paquets. Qualité de service, assemblage, reprise sur perte de message, Contrôle de Flux Transporte des unités de données appelées messages. Protocole TCP et UDP et TCP / IP.

e. **Couche Session :** La couche 5 du modèle OSI correspond à la couche session, également qualifiée de « couche de contrôle des communications ». Elle s'occupe de fiabiliser la communication utilisateurs, gère des tours de parole, synchronisation. Synchronisation du Dialogue.

f. **La couche présentation :** La couche présentation définit un format des données par lequel les informations circuleront dans le réseau. Les données de la couche présentation sont adaptées à un format uniforme pour que tous les ordinateurs concernés puissent les traiter. Cela est nécessaire car les plates-formes PC, Macintosh ou les différents UNIX représentent les données de manière différente. Il convient donc d'adopter une représentation unique si nous souhaitons que ces plates-formes puissent communiquer.

g. **La couche application :** La couche application est la couche supérieure du modèle OSI et donne accès aux services réseau de l'ordinateur. Elle comprend des programmes tels que le navigateur qui permet à l'utilisateur de lire des pages Web, le client FTP (File Transfer Protocol) pour le téléchargement de fichiers, le programme de messagerie, les applications de bases de données et de nombreux autres logiciels qui nécessitent un accès réseau.

3. La couche physique

Dans ce qui va suivre, nous allons parler de la première couche du modèle OSI : la couche physique. Pour rappel, cette couche physique s'occupe de la transmission physique des données entre deux équipements réseaux. Elle s'occupe de tout ce qui a trait au bas-niveau, au matériel : la transmission des bits, leur encodage, etc. Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.

Les informations à transmettre étant des 0 et 1, on peut imaginer transmettre sur la voie physique un signal "carré" avec une tension différente pour les 0 et les 1. Or le support physique altère facilement les signaux carrés. Tant que le débit et la distance à parcourir sont faibles, on peut utiliser un signal carré, mais on est amené à mettre en œuvre des techniques plus sophistiquées pour améliorer les performances.

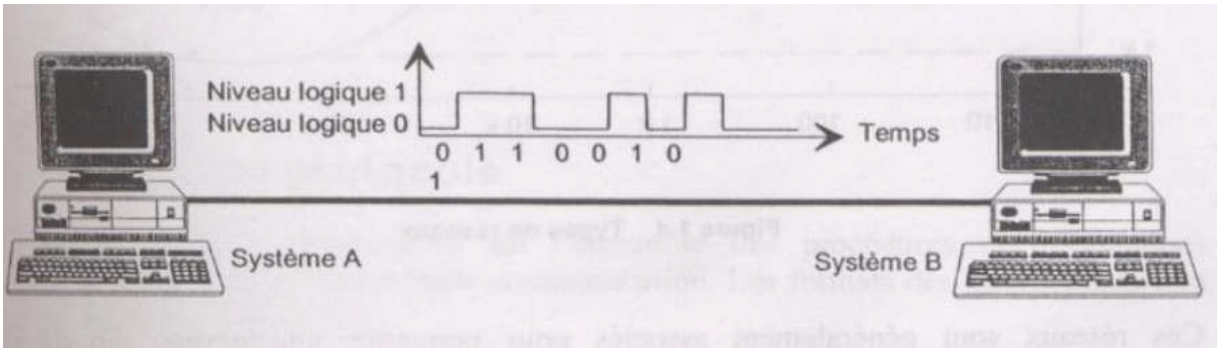


Fig.2. Transmission numérique entre deux systèmes.

3.1. Transmission de l'information

La transmission utilise un signal basé sur le principe de propagation d'ondes : ondes électriques (câbles, files), ondes radio (faisceau hertzien, satellites), ondes lumineuses (fibres optiques).

L'étude de la transmission de l'information nécessite la connaissance :

- Des principes du signal
- Des supports de transmission et leurs caractéristiques ;
- Des méthodes utilisées pour transmettre l'information sur ses supports.

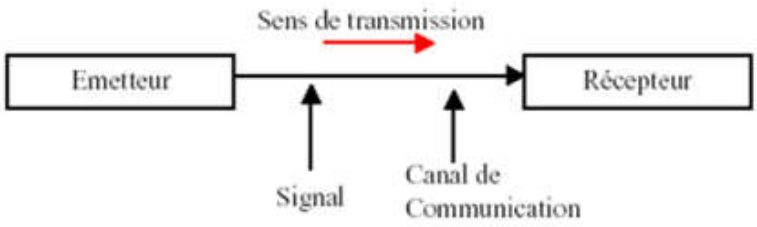


Fig.3. Transmission de l'information entre deux systèmes.

3.1.1. Notion de signal

Un signal est une variation de tension, impulsion lumineuse, modulation d'une électromagnétique, etc.

Signal périodique : se reproduit de façon identique dans le temps, et se caractérisé par une période T (en second) et une fréquence F = 1/T (en Hertz).

Signal analogique : Un signal analogique est un signal continu qui peut prendre une infinité de valeurs (proportionnel à la valeur de l'information : son, image …).

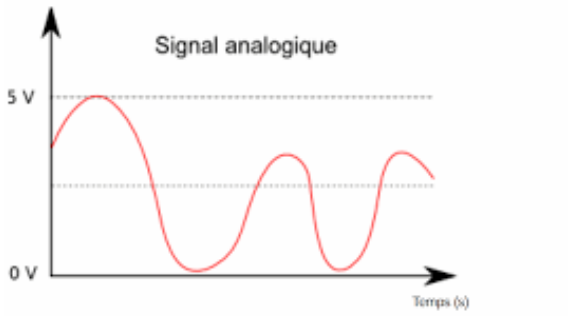


Fig.4. Signal analogique.

Signal numérique : Un signal numérique est un signal discret (discontinu), qui se résume en une succession de « 0 » et de « 1 ».

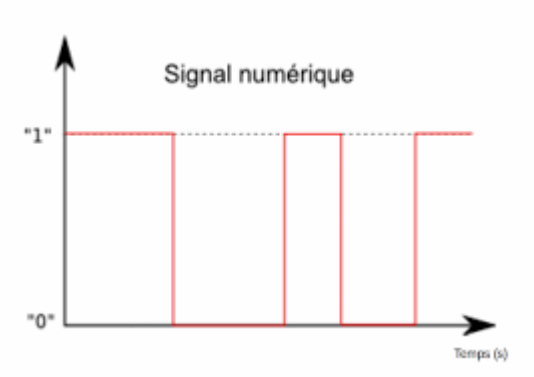


Fig.5. Signal numérique.

3.2. Caractéristiques des supports de transmission

Un support physique de transmission peut être de nature très diverse : paire de fils métalliques, câble coaxial, fibre optique, atmosphère …etc. , il est caractérisé par les effets indésirables qu'il exerce sur les signaux qui le traversent . Certains de ces effets sont dus à la nature même du support de transmission d'autres sont dus à l'environnement externe.

Les caractéristiques des supports de transmission (débit, taux d'erreurs) dépendent de la bande passante, et de l'affaiblissement du signal … etc, et de la façon d'utiliser le support pour transmettre des données (multiplexage ou non, …).

a. **Bande Passante (BP):** La largeur de la bande passante est la caractéristique essentielle d'un support de transmission, qui se comporte généralement comme un filtre qui ne laisse donc passer qu'une bande limitée de fréquence appelée bande passante. Toute fréquence en dehors de cette bande sont fortement affaiblie.

   Exemple: une ligne téléphonique ordinaire ne laisse passer que les signaux de fréquence comprise entre 300 Hz et 3400 Hz. Au dehors de cette bande les signaux sont fortement atténués et ne sont plus compréhensible, on dit alors que la bande passante d'une telle ligne est de 3400–300 Hz soit 3100 Hz.

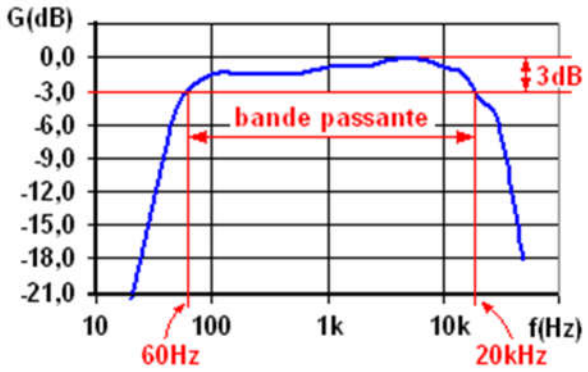


Fig.6. La bande passante.

b. **La rapidité de modulation maximal:** Le nombre maximal de modulation (changement d'états) d'un signal par unité de temps est lié à la bande passante du support de transmission par le critère de Nysquist

$$R_{max} \leq 2*BP$$

Où BP est la bande passante et R_{max} la rapidité de modulation maximal.

c. **Rapidité de modulation :** La rapidité de modulation ou bien débit de symbole exprimée en bauds correspond au nombre d'intervalles de modulation ou de symboles par seconde. La rapidité de modulation R d'un signal est défini par la relation suivant :

$$R\ (Baud) = (1/\Delta)$$

Ou Δ présent le temps pendant lequel les caractéristiques du signal à transmettre ne sont pas modifiées.

d. **Capacité :** Quantité d'information pouvant être transmise en une seconde. S'exprime en bit/s. Le débit binaire **maximum** ou capacité C d'une ligne de transmission peut être défini suivant les caractéristiques de la ligne par la relation :

$$C\ (Bit/s) = BP\ log_2\ (1+S/B)$$

Ou C la capacité (en bit/s), BP est la bande passante du support (en Hz) et S/B est le rapport signal sur bruit sans unité (il est exprimé en valeur et non en dB).

e. **Débit binaire (D):** C'est la quantité d'informations par unité de temps émise à la source. Son Unité est (bit/s), est calculé par cette relation :

$$D\ (Bit/s) = R\ Log_2\ (V)$$

V est la valence, présent le nombre d'états significatifs distincts employés dans une modulation pour caractériser les éléments du signal à transmettre.

f. **Affaiblissement:** Un canal de transmission atténue (affaiblit) l'amplitude du signal qui le traverse. Le phénomène d'atténuation correspond à une perte d'énergie du signal pendant sa propagation sur le canal et s'accentue avec la longueur de celui-ci. La quantité d'énergie perdue dépend très étroitement de la fréquence du signal et de la bande passante du système. On mesure l'atténuation par le rapport Ps/Pe où Ps est la puissance du signal à la sortie du canal et Pe la puissance du signal à l'entrée du canal. Il est courant d'exprimer l'atténuation en décibels (dB) sous la forme:

$$A(dB) = 10log_{10}(Ps/pe)$$

g. **Le bruit :** Le bruit est un signal perturbateur provenant du canal lui-même ou de son environnement externe. Il est de comportement aléatoire est vient s'ajouter au signal véhiculant les informations et provoquer ainsi les erreurs de transmission.
La quantité de bruit présente sur un canal de transmission, est exprimé par le rapport de la puissance du signal transmis sur la puissance de bruit et prend le nom de rapport signal sur bruit, nous écrivons ce rapport :

$$N(dB) = 10\ log_{10}(S/B)$$

Ce rapport varie dans le temps, puisque le bruit n'est pas uniforme, toutefois on peut en estimer une valeur moyenne sur un intervalle de temps. Le rapport signal sur bruit est aussi une caractéristique d'un canal de transmission.

h. **Le temps de propagation :** est le temps nécessaire à un signal pour parcourir un support d'un point à un autre, ce temps dépend donc de la nature du support, de la distance et également de la fréquence du signal.

Temps de propagation (T_p) :

$$T_p = distance / vitesse\ de\ propagation$$

i. **Le temps de transmission ou d'émission:** est le délai qui s'écoule entre le début et la fin de la transmission d'un message sur une ligne, ce temps est donc égal au rapport entre la longueur du message et le débit de la ligne.

Temps de transmission ou d'émission (Te) :

$$Te = longueur\ du\ message / vitesse\ de\ transmission = Q / D$$

j. **Temps de transfert:** ou délai d'acheminement sur une voie est égal au temps total mis par un message pour parvenir d'un point à un autre, c'est donc la somme des temps de propagation et temps d'émission :

$$T_{tr} = T_t + T_p$$

Pour évaluer l'importance relative du temps de propagation T_p, il est nécessaire de comparer celui-ci au temps de transmission du message sur la ligne.

3.3. Méthodes de transmission

3.3.1. Transmission en bande de base

Lorsque la longueur de la liaison ne dépasse pas quelques centaines de mètres, les informations peuvent être transmises sur le support de liaison sans transformation du signal numérique en signal analogique.

En général, le signal binaire n'est pas transmis directement sur la ligne. Les codages en bande de base vont essentiellement avoir pour rôle de diminuer la largeur de bande du signal binaire et de transposer celle-ci vers des fréquences plus élevées. La carte réseau intégrée dans le PC ou le routeur, qui réalise ce codage en bande de base. Différents codages numériques sont utilisés :

a. Codage NRZ (No Return to Zero)

Le signal binaire est simplement transposé en tension pour éviter une composante continue non nulle.

Exemple : Le codage NRZ de la séquence de bits 1110 0001 1011 est représenté dans la figure 7.

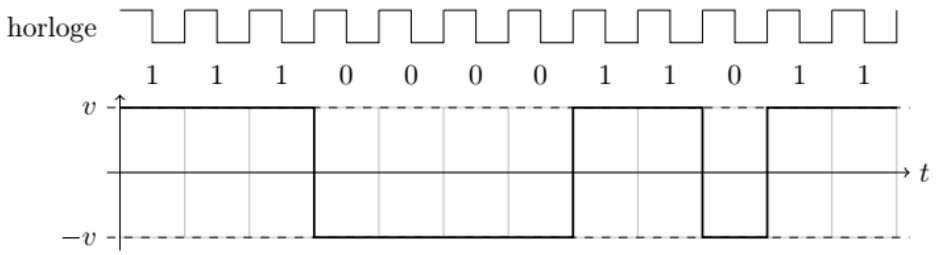


Fig.7. Le codage NRZ.

b. Codage NRZI (No Return to Zero Inverted)

Présente les mêmes caractéristiques de codage NRZ mais pour éviter les successions de 0, le signal reste dans le même état pour coder un 0 (le niveau précédent est conservé) et on change l'état pour coder un 1.

Exemple : Le codage NRZI de la séquence de bits 1110 0001 1011 est représenté dans la Figure 8, en supposant que le niveau précédent était +v.

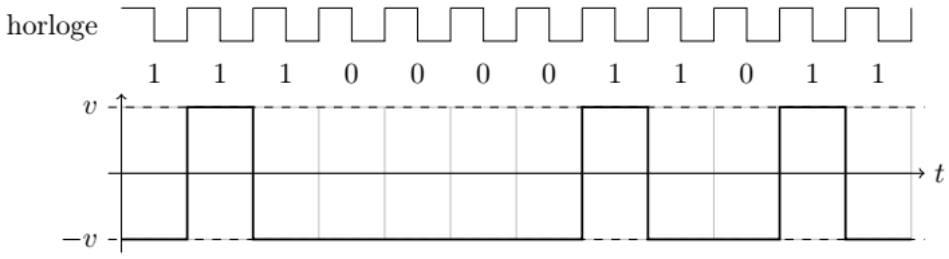


Fig.8. Le codage NRZI.

c. Codage Manchester

Pour augmenter les changements d'états, une transition systématique est réalisée au milieu de chaque bit du signal binaire : une transition négative lorsque le signal binaire est à 1 et une transition positive lorsque le signal binaire est à 0 (Un bit 1 est transformé en deux bits 10, et un bit 0 est transformé en 01).

Exemple : Le codage Manchester de la séquence de bits 1110 0001 1011 est représenté dans la figure 9.

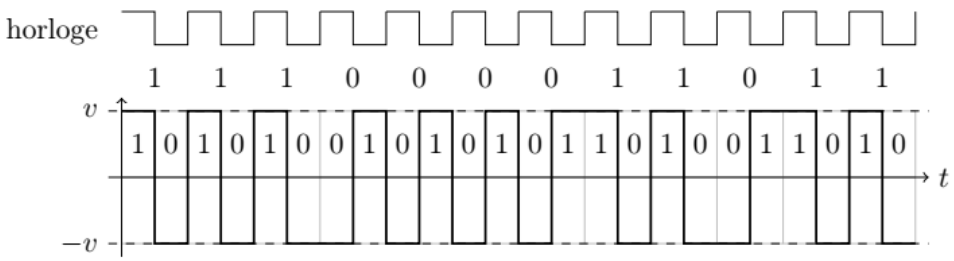


Fig.9. Le codage Manchester.

d. Codage Manchester différentiel

Une transition systématique est réalisée au milieu de chaque bit. Pas de transition pour coder un bit à 1, une transition pour coder un bit à 0.

Exemple : Le codage Manchester différentiel de la séquence de bits 1110 0001 1011 est représenté dans la figure 10.

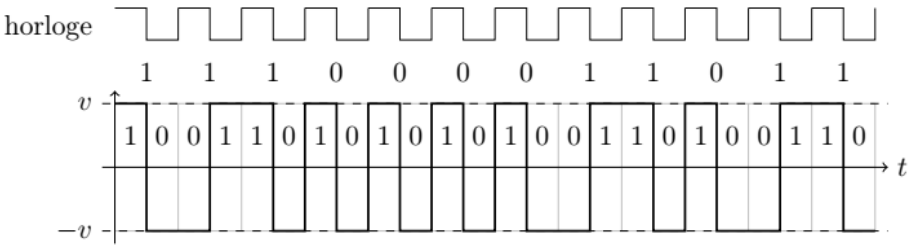


Fig.10. Le codage Manchester différentiel.

e. Codage Miller ou Delay Mode

Une transition au milieu du bit pour un 1, pas de transition en milieu de bit pour un 0. Une transition à la fin du bit pour un 0 si le bit suivant est aussi un 0.

Exemple: Le codage Miller de la séquence de bits 01001100100 est représenté dans la figure 11.

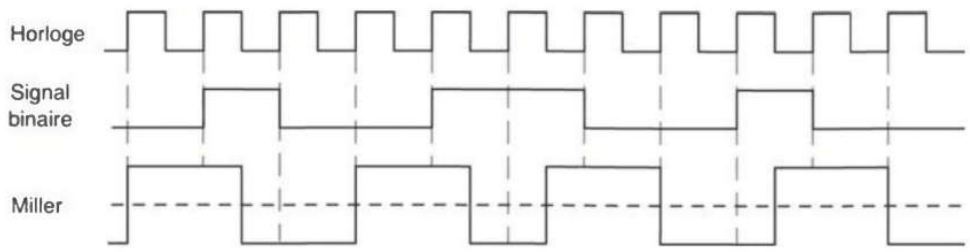


Fig.11. Le codage Miller.

3.3.2. Transmission large bande (Modulation/démodulation)

Pour transmettre l'information à longue distance, on module une onde porteuse sinusoïdale.

Mathématiquement, elle est de la forme : s(t) = A.sin(ω.t + Φ) A : Amplitude , ω : Pulsation , Φ : Phase initiale ou :

$$s(t) = A.sin\ (2\pi f.t + \Phi)$$ f : Fréquence

Les types de modulation

a. Modulation d'amplitude : Le signal est modulé en faisant varier l'amplitude.

$$s(t) = A(t)\ .\ sin(\omega.t + \Phi)$$

Cette technique est efficace si la bande passante et la fréquence sont bien ajustées par contre, il existe des possibilités de perturbation (orage, lignes électriques.) car si un signal de grande amplitude (représentant un 1) est momentanément serais affaibli le récepteur l'interprétera à tort en 0.

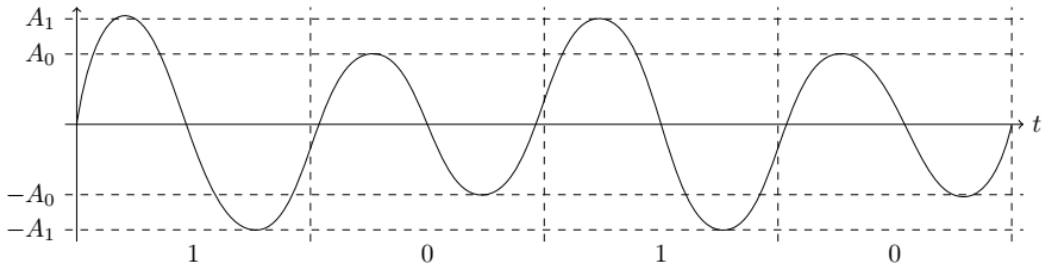


Fig.12. Exemple de modulation d'amplitude.

b. Modulation de fréquence : $s(t) = A \cdot \sin(2\pi f(t).t + \Phi)$, c'est un signal très résistant aux perturbations (la radio FM est de meilleur qualité que la radio AM) et c'est assez facile à détecter.

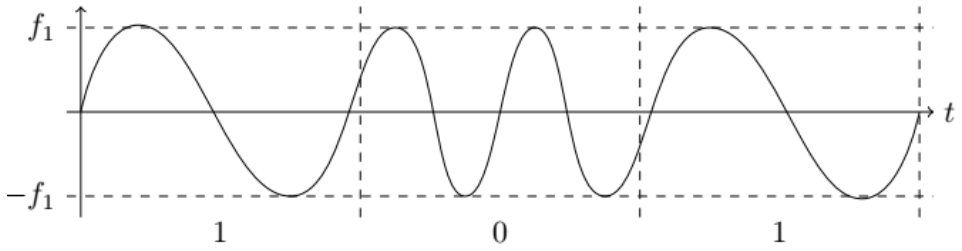


Fig.13. Exemple de modulation de fréquence.

c. Modulation de phase : $s(t) = A. \sin(2\pi f.t + \Phi(t))$

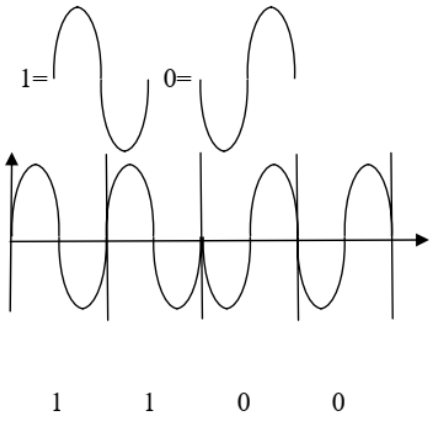


Fig.14. Exemple de modulation de phase.

4. Couche liaison de données

L'information échangée entre deux ETTD (Equipement Terminal de Traitement de Données) peut subir certains erreurs provoquées par les supports de transmission ou par l'anomalie des équipements physiques d'interconnexion (commutateurs, concentrateurs, … etc.). Ces erreurs peuvent être quantifiées en termes d'un taux, dit taux d'erreur.

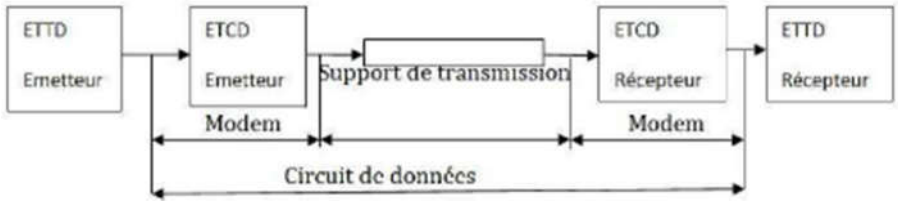


Fig.15. Représentation la couche de liaison des données.

Celui-ci est donné par le rapport :

$$taux\ d'erreur = \frac{Nombre\ de\ bits\ erronés}{Nombre\ de\ bits\ émis}$$

L'impact des erreurs sur l'information est se traduit par l'inversement de certains bits ce qui peut mener à :

- ***La corruption de l'information :*** le récepteur pour recevoir une information erronée.
- ***La perte de l'information :*** le récepteur ne peut rien recevoir si l'erreur infecte la séquence qui indique le début de la séquence d'information (la non-reconnaissance de la séquence).

4.1. Méthodes de protection contre les erreurs de transmission

On vue que le bruit environnant et le bruit blanc exercent des effets indésirables sur les données transmises, pouvaient se traduire au niveau liaison par l'altération, la perte ou même la duplication de trames.

Le rôle d'un protocole de liaison est de masquer les défauts du support de transmission afin d'assurer un transfert des données avec un taux d'erreurs négligeables.

On distingue deux méthodes de protection contre les erreurs:

- Les méthodes de protection pour la détection.
- Les méthodes de protection pour la correction

4.1.1. Méthodes de détection des erreurs

Pour ce type de protection l'information de redondance doit être déterminée de manière telle que le récepteur puisse seulement détecter les erreurs de transmission, la correction se fera dans une seconde phase, par le biais de technique de retransmission.

a. la parité transversale (VRC : Vertical Redundancy Check)

A chaque caractère de 7 bits on ajoute un bit de contrôle, dit de parité, indiquant si le nombre de bit à 1 est pair ou impair. Si ce nombre est pair, on ajoute 0 sinon, on ajoute 1.

Pour détecter la présence des erreurs, le récepteur procède comme suite : pour chaque (7 bits de) caractère, il recalcule la parité et compare le résultat avec la valeur du 8ème bit. Il n'y aura pas d'erreur si la parité calculé est identique à celle émise.

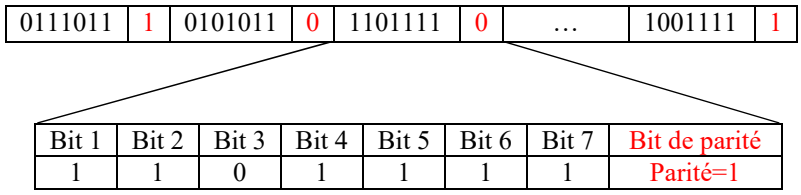


Fig.16. Calcul du bit de parité.

b. Méthode basée la parité transversale et longitudinale (LRC : Longitudinal Redundancy Check)

La méthode consiste à protéger chaque caractère par une parité transversale, mais également à protéger chaque colonne au niveau de la trame par une parité longitudinale. On considère l'information à transmettre comme une matrice (chaque ligne est un caractère) et on calcule la parité verticalement (longitudinalement) et horizontalement (transversalement).

Pour détecter la présence des erreurs, le récepteur procède comme suite : pour chaque (7 bits) de ligne et pour (n-1) bits de chaque colonne, il compare la parité recalculée avec la parité émise dans le message. Il n'y aura pas d'erreur si la parité calculé est identique à celle émise.

L'inconvénient de cette méthode de protection est quelle est inefficaces en cas d'occurrence d'erreurs groupées.

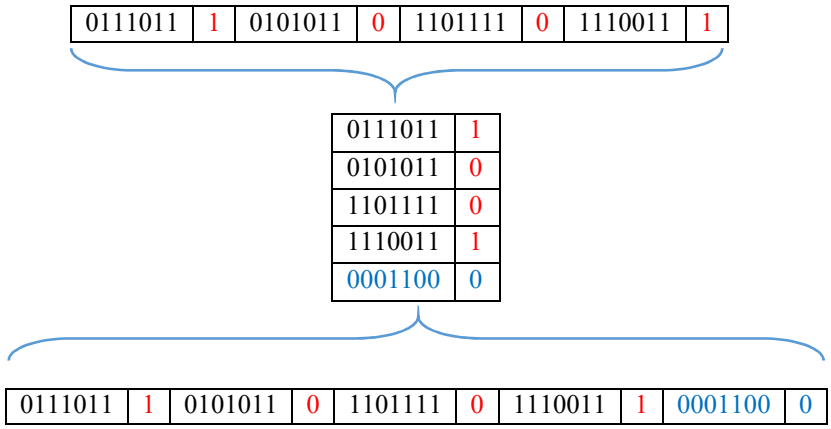


Fig.17. Calcul des bits de parité transversale et longitudinale.

c. Méthode basée sur le code générateur (code à redondance cycliques ou CRC)

Dans le cas des méthodes basées sur la parité, l'information de contrôle est composée des bits de parité. Cette méthode génère l'information de contrôle en effectuant une division d'un polynôme extrait de l'information par un autre polynôme dit générateur.

Trouver le polynôme associé à une séquence de bits : Soit I une séquence de bits : $b_1, b_2, b_3, \ldots b_k$, le polynôme y associé est $I(x) = b_1 \times x^{k-1} + b_2 \times x^{k-2} + b_3 \times x^{k-3} + b_4 \times x^{k-4} + \ldots + b_k$. (Tous les coefficients du polynôme sont 0 ou 1).

Exemple:

$I = 1101 \rightarrow 1 \times x^3 + 1 \times x^2 + 0 \times x + 1 = x^3 + x^2 + 1$

$I = 110001 \rightarrow 1 \times x^5 + 1 \times x^4 + 0 \times x^3 + 0 \times x^2 + 0 \times x + 1 = x^5 + x^4 + 1$

$I = 1101011011 \rightarrow 1 \times x^9 + 1 \times x^8 + 0 \times x^7 + 1 \times x^6 + 0 \times x^5 + 1 \times x^4 + 1 \times x^3 + 0 \times x^2 + 1 \times x + 1 = x^9 + x^8 + x^6 + x^4 + x^3 + x + 1$

- **Coté émetteur :** soit la séquence des bits à envoyer, on calcule le reste de la division, soit $R(x)$, (qu'on appelle CRC) du polynôme x^n. $I(x)$ par un polynôme dit générateur $G(x)$ de degré n. Alors, la séquence M à envoyer est celle correspondant au polynôme $M(x) = x^n . I(x) + R(x)$.
- **Coté récepteur :** Pour détecter la présence des erreurs, le récepteur procède comme suite : on divise le polynôme correspondant à la séquence de bits reçus $M(x)$, soit par le polynôme

générateur (celui utilisé par l'émetteur). La séquence reçue est jugée correct si le reste de la division est nul ($R = 0$). Sinon, elle est jugé erronée.

L'émetteur et le récepteur utilisent tous les deux un polynôme générateur *G(x)* (qui est constant).

Ce polynôme *G(x)* va servir :

- à l'émetteur pour d´exterminer les bits qui seront effectivement transmis ;
- au récepteur pour déterminer si la transmission s'est déroulée sans erreur

4.1.2. Méthodes de protection pour la correction

Les méthodes de détection présentées dans la section précédente permettent au récepteur de détecter l'existence des erreurs sans pouvoir les localiser. Par conséquence, elles ne permettent pas les corriger.

Pour corriger les erreurs, il y a lieu d'envisager des techniques de retransmission complémentaires. Ces méthodes sont appelés méthodes de retransmission automatiques (*ARQ automatique repeat request*):

a. Transmission avec arrêt et attente

À la réception d'une trame d'information correcte par le récepteur, il renvoie à l'émetteur une trame d'acquittement (un accusé de réception), une trame d'acquittement de taille relativement courte.

Un délai de garde est armé à l'émission si à l'expiration du délai pas d'acquittement reçu, alors l'émetteur suppose que la trame perdue. Même en cas de perte d'acquittement, il y aura une retransmission de la trame plusieurs fois, au bout d'un nombre limité de retransmission, la liaison est supposée défaillante, la couche supérieur est informée.

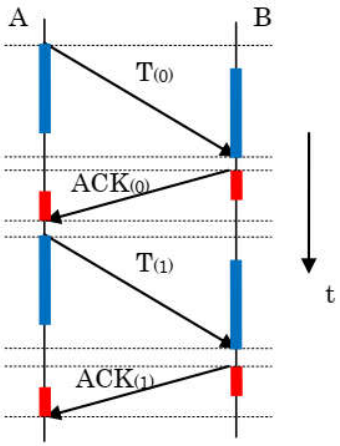


Fig.18. Scénario de Transmission avec arrêt et attente.

b. Transmission continue

Dans ce mode de transmission continue, l'émetteur reste inactif lors de l'attente de l'acquittement. Pour éviter ce problème, une autre solution consiste à exploiter le temps d'attente d'un acquittement pour envoyer une autre trame d'information. Il s'agit de la transmission continue.

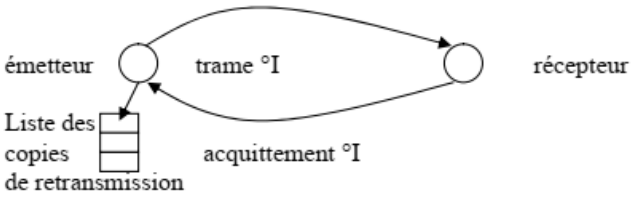


Fig.19. Scénario de transmission continue.

Dans les méthodes de transmission continue, l'émetteur peut envoyer plusieurs trames en attendant un acquittement. Pour gérer la transmission, l'émetteur garde une copie de chaque trame émise jusqu'à la réception de l'acquittement correspondant.

Si certaine trame de l'ensemble des trames émises est perdue ou erronée, l'émetteur va procéder à la retransmission de cette trame et continue la transmission normalement : Retransmission sélective ou continue la transmission des trames venant après cette trame: retransmission systématique (GO-BACK-N).

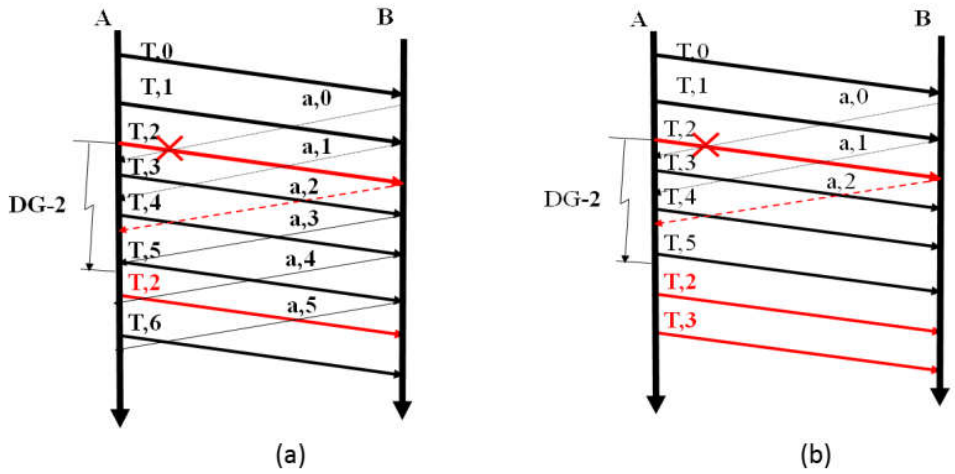


Fig.20. Scénarios de retransmission. (a) retransmission sélective; (b) retransmission systématique.

Comparaison entre retransmission Sélective et systématique : la comparaison des deux types de retransmission est résumée dans le tableau ci-dessous :

Critères de comparaison	**Retransmission systématique**	**Retransmission Sélective**
Implémentation	Simple	Complexe
Efficacité	Peu efficace	Plus efficace
Consommation de mémoire	Pas besoin de Mémorisation des trames côté récepteur	Mémorisation des trames côté récepteur

5. Couche réseau

Le rôle de la couche réseau est de transporter des paquets d'un nœud à un autre nœud connecté au même réseau. Ce niveau 3 (réseaux) réalise trois fonctions principales.

- ✓ Le contrôle de flux et l'évitement de congestion : Le contrôle de flux permet l'évitement des congestions dans le réseau.
- ✓ Le routage : permet d'acheminer les paquets d'informations vers leurs destinations (peut être centralisé ou distribué).
- ✓ L'adressage : représente l'ensemble des moyens permettant de désigner un élément dans un réseau.
- ✓ Et en plus la détection des erreurs qui ne sont pas détecter par la couche liaison.

5.1. Le contrôle de flux (de réseau)

Consiste à gérer les paquets pour qu'ils transitent le plus rapidement possible entre l'émetteur et le récepteur, il cherche à éviter les problèmes de congestion du réseau qui surviennent lorsque trop de message circulent dedans, on peut citer quelques méthodes :

- ***Le contrôle par crédit :*** seuls N paquets sont autorisés à circuler simultanément sur le réseau, donc un paquet ne peut entrer dans le réseau qu'après avoir acquis un jeton qu'il relâche lorsqu'il arrive à destination.
- ***Le contrôle par jeton dédié :*** cette technique améliore la précédente en imposant au jeton de retourner à l'émetteur et à l'émetteur de gérer une file d'attente des paquets émis.
- ***Le mécanisme de la fenêtre :*** dans le cadre d'un circuit virtuel établi entre l'émetteur et le récepteur, les paquets sont numéroté modulo 8 et contiennent que deux compteur P(s) et P(r), l'émetteur n'est autorisé à émettre que les paquets inclus dans la fenêtre w, tel que l'inégalité suivante soit vérifiée.

5.2. Le Routage

Le routage des paquets dans un réseau maillé consiste à fixer par quelle ligne de sortie chaque commutateur réexpédie les paquets qu'il reçoit. Ceci se fait en fonction de la destination finale du paquet et selon une table de routage qui indique pour chaque destination finale quelles sont les voies de sortie possible.

5.2.1. Principe de routage

La Fig.29 illustre un réseau composé de 4 machines, M1, M2, M3, M4, regroupées en deux sous-réseaux reliés par un routeur.

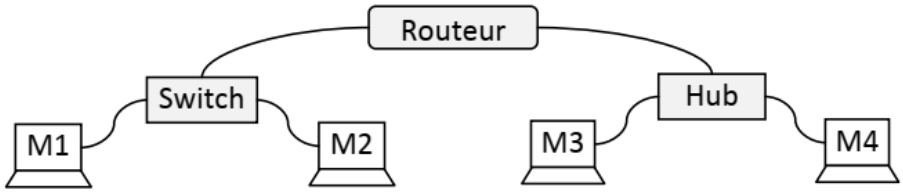


Fig.21. Interconnexion de deux réseaux physiques.

On distingue deux cas :

Cas 1 : la machine source et destinataire se trouvent sur le même réseau physique : Dans ce cas, la machine source envoi la trame (respectivement le paquet) à l'adresse Mac (respectivement l'adresse IP) de la machine destinataire

Si on supposant que la machine M1 va transmettre un message à la machine M2.

- l'adresse IP source et destinataire du paquet à émettre à M2 sont respectivement celle de M1 et celle de M2.
- l'adresse Mac source et destinataire de la trame encapsulant ce paquet sont respectivement celle de M1 et celle de M2.

Dans ce cas le comportement du routeur n'a aucun effet sur l'acheminement car les deux stations source et destinataire se trouvant sur le même réseau physique (même fragment).

Cas 2 : la machine source et destinataire se trouvent sur des sous réseaux différents (interconnectés par un ou plusieurs routeurs) : Dans ce cas, la station source envoi la trame (respectivement le paquet) à l'adresse Mac (respectivement l'adresse IP) du routeur (respectivement de la station destinataire)

Si on supposant que la machine M1 va transmettre un message à la machine M3.

- l'adresse IP source et destinataire du paquet à émettre à M3 sont respectivement celle de M1 et celle de M3.
- l'adresse Mac source et destinataire de la trame encapsulant ce paquet sont respectivement celle de M1 et celle de Routeur.

Dans ce cas le routeur se comporte comme passerelle entre le sous-réseau contenant M1 et celui contenant M3. Comme l'acheminement s'effectue sur la couche réseau (ou Internet) la couche liaison du routeur doit avoir le droit de recevoir la trame à acheminer. Une raison pour laquelle l'adresse Mac destinataire doit être celle du Routeur.

5.3. Adressage

Sur Internet, de nombreux protocoles sont utilisés, ils font partie d'une suite de protocoles qui s'appelle TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP est basé sur le repérage de chaque ordinateur par une adresse appelée adresse IP qui permet d'acheminer les données à la bonne adresse.

Chaque paquet transmis via le protocole IP contient dans son en-tête l'adresse IP de l'émetteur ainsi que l'adresse IP du destinataire. Cela permet aux machines du réseau de router les paquets jusqu'à destination grâce à l'adresse IP. Le destinataire saura ainsi à qui renvoyer les données grâce à l'adresse IP de l'émetteur contenu dans les en-têtes des paquets envoyés.

5.3.1. Adresse IP

Une adresse IP est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. Cette adresse est le numéro unique d'un ordinateur ou d'une machine sur un réseau qui lui permet de communiquer sur ce réseau.

L'adresse IP (IPv4) est formée de 4 octets (32 bits), compris entre 0 et 255 (sous forme décimale), séparés par un point (notation décimale pointée) comme la montre la figure ci-dessous :

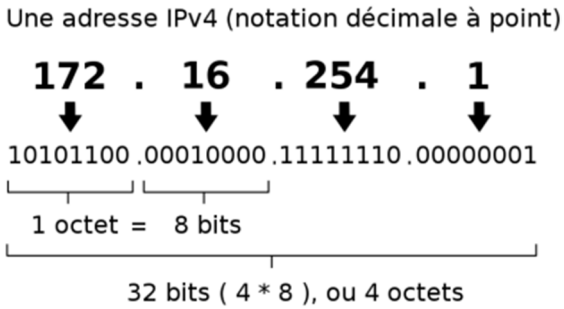


Fig.22. L'adresse IP.

5.3.2. Classe d'adresses IP

Une adresse IP est composée d'une partie fixe servant à identifier le réseau (Net id) et une partie servant à identifier une machine (hôte) sur ce réseau (Host id). On dénombre 3 grandes classes d'adresses IP. Sur le tableau ci-dessous, les adresses réseaux sont en gras et les adresses machines en italique :

Classe A	**Octet n°4**	*Octet n°3*	*Octet n°2*	*Octet n°1*
Classe B	**Octet n°4**	**Octet n°3**	*Octet n°2*	*Octet n°1*
Classe C	**Octet n°4**	**Octet n°3**	**Octet n°2**	*Octet n°1*

- **Classe A :** Dans une adresse IP de classe A, le premier octet représente le réseau. Les réseaux disponibles en classe A sont donc les réseaux allant de 1.0.0.0 à 126.0.0.0 (les derniers octets sont des zéros ce qui indique qu'il s'agit bien de réseaux et non d'ordinateurs) ;
- **Classe B :** Dans une adresse IP de classe B, les deux premiers octets représentent le réseau. Les deux premiers bits sont 1 et 0, ce qui signifie qu'il y a 2^{14} possibilités de réseaux, soit 16382 réseaux possibles. Les réseaux disponibles en classe B sont donc les réseaux allant de 128.0.0.0 à 191.254.0.0 ;
- **Classe C :** Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1,1 et 0, ce qui signifie qu'il y a 2^{21} -2 possibilités de réseaux, c'est-à-dire 2097150. Les réseaux disponibles en classe C sont donc les réseaux allant de 192.0.0.0 à 223.255.254.0. L'octet de droite représente les ordinateurs du réseau, le réseau peut donc contenir: 2^8-2^1 = 254 ordinateurs.

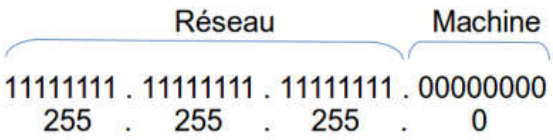
5.3.3. Masque réseau ou masque sous-réseau

En 1984, devant la limitation du modèle de classes, la RFC 9174 (Internet Subnets) crée le concept de sous-réseau qui introduit un niveau hiérarchique supplémentaire entre le numéro de réseau et le numéro d'hôte. Ceci permet par exemple d'utiliser une adresse de Classe B comme 256 sous-réseaux de 254 ordinateurs au lieu d'un seul réseau de 65534 ordinateurs, sans toutefois remettre en question la notion de classe d'adresse. Ceci permet plus de flexibilité et d'efficacité dans l'attribution des adresses.

a. ***Un sous-réseau*** : Une subdivision logique d'un réseau de taille plus importante. Un sous-réseau correspond typiquement à un réseau local sous-jacent. La création des sous réseaux permet de :

- ✓ Bien structurer le réseau global ;
- ✓ Améliorer les performances du réseau (limiter l'effet de la diffusion et de la collision)

b. ***Masque :*** Le masque est un séparateur entre la partie réseau et la partie machine d'une adresse IP. Le masque, comme l'adresse IP, est une suite de 4 octets, soit 32 bits. Chacun de ces bits peut prendre la valeur 1 ou 0. Pour définir le masque, il nous suffit de dire que les bits à 1 représenteront la partie réseau (Net-ID) de l'adresse, et les bits à 0 la partie machine (Host-ID). Ainsi, on fera une association entre une adresse IP et un masque pour savoir, dans cette adresse IP, quelle est la partie réseau et quelle est la partie machine de l'adresse.



Ainsi, dans l'exemple ci-dessus, il nous reste 8 bits à 0, on aura donc la possibilité d'avoir 2^8 machines disponibles dans ce sous-réseau, machines qui pourront dialoguer entre-elles.

Dans le cas où les adresses sont déterminées selon une classe des trois classes A, B et C, le masque est dit "masque par défaut". Le tableau suivant indiqué donc le masque pour chacune des classes:

Classe	Masque par défaut
Classe A	255. 0. 0.0
Classe B	255. 255. 0.0
Classe C	255. 255. 255.0

c. Association adresse IP et masque :

Nous avons vu que l'adresse IP doit être obligatoirement associé à un masque. Prenons par exemple une machine qui a pour adresse IP (192.168.25.147). Il nous faut lui associer un masque pour savoir quelle partie de cette adresse représente le réseau. Associons-lui le masque 255.255.255.0.

On remarque que les bits des trois premiers octets sont à 1, ils représentent donc la partie réseau de l'adresse, soit 192.168.25, le 147 permettant d'identifier la machine au sein de ce réseau.

Dans cet exemple, on remarque qu'un octet (le dernier) a été réservé pour l'adresse machine, ce qui nous donne $2^8 = 256$ adresses disponibles pour les machines sur le réseau 192.168.25. Les adresses disponibles pour les machines seront donc :

192.168.25.0 (réservée pour le réseau, à ne pas utiliser)
192.168.25.1
...
192.168.25.147
...
192.168.25.254
192.168.25.255 (réservée pour le broadcast, à ne pas utiliser)
On observe donc que c'est le masque qui détermine le nombre de machines d'un réseau. Ainsi, on choisira le masque en fonction du nombre de machines que l'on veut installer dans notre réseau !

Adresse de réseau : L'adresse de réseau permet de savoir si 2 machines peuvent communiquer entre elles. Si ces 2 machines ont une adresse réseau identique, alors, elles appartiennent au même réseau et elles peuvent communiquer. L'adresse réseau se calcule en utilisant l'équation logique suivante :

Adresse réseau = Adresse IP ET Masque de sous-réseau

ET est l'opérateur logique (AND) en binaire, dont voici la table de vérité correspondante :

Table de vérité de ET ou AND		
Adresse IP	Masque	Adresse réseau
0	0	0
0	1	0
1	0	0
1	1	1

Exemple :

Soit l'adresse IP suivante : 192.168.0.10/24. Le calcul de l'adresse réseau donne :

Ip	11000000.10101000.00000000.00001000
ET	
Masque	11111111.11111111.11111111.00000000
=	11000000.10101000.00000000.00000000

Soit 192.168.0.0, écrit sous forme décimale pointée.

5.3.4. Adressage privé et public

Un adressage privé est un adressage où les adresses affectées aux machines doivent être complètement séparées de celles de l'Internet.

Contrairement à l'adressage privé, l'adressage public implique l'obtention des adresses des "organismes de régulation de l'Internet". L'obtention de ces adresses nécessite une justification de leur usage auprès de ces organismes.

Le choix entre un adressage privé et public n'a aucune importance que dans le cas où le réseau est interconnecté à un internet. Le problème qui se pose dans ce cas est celui de conflit des adresses internes avec et celles de l'Internet.

Les adresses privées par classe sont résumés dans le tableau suivant :

Classe	Plage d'adresses	Masque de réseau
Classe A	10.0.0.0 - 10.255.255.255	10.0.0.0
Classe B	172.16.0.0 - 172.31.255.255	172.16.0.0
Classe C	192.168.0.0 - 192.168.255.255	192.168.0.0